Accepting Blame: Expressive Checked Exceptions

Yizhou Zhang* Guido Salvaneschi† Quinn Beightol*
Barbara Liskov‡ Andrew C. Myers*

*Cornell University †TU Darmstadt ‡MIT
yizhou@cs.cornell.edu salvaneschi@cs.tu-darmstadt.de qeb2@cornell.edu
liskov@csail.mit.edu andru@cs.cornell.edu

April 15, 2016

Unhandled exceptions crash programs, so a compile-time check that exceptions are handled should in principle make software more reliable. But designers of some recent languages have argued that the benefits of statically checked exceptions are not worth the costs. We introduce a new statically checked exception mechanism that addresses the problems with existing checked-exception mechanisms. In particular, it interacts well with higher-order functions and other design patterns. The key insight is that whether an exception should be treated as a “checked” exception is not a property of its type but rather of the context in which the exception propagates. Statically checked exceptions can “tunnel” through code that is oblivious to their presence, but the type system nevertheless checks that these exceptions are handled. Further, exceptions can be tunneled without being accidentally caught, by expanding the space of exception identifiers to identify the exception-handling context. The resulting mechanism is expressive, syntactically light, and can be implemented efficiently. We demonstrate the expressiveness of the mechanism using significant codebases and evaluate its performance. We have implemented this new exception mechanism as part of the new Genus programming language, but the mechanism could equally well be applied to other programming languages.

1 Introduction

Exceptions make code more reliable by helping programmers handle abnormal or unusual run-time conditions. The core idea is to transfer control in a nonlocal way to handler code that can be factored out from common-case code. This separation of concerns simplifies code and prompts programmers not to forget about exceptional conditions.

There has been disagreement since the 1970’s about how or whether exceptions should be subject to static checking [Goodenough 1975; MacLaren 1977]. This disagreement continues to the present day [Goetz 2004]. Some currently popular languages—Java [Gosling et al. 2005] and Swift [Swift 2014]—offer checked exceptions that the compiler statically ensures are handled. However, exceptions are not part of type checking in other popular languages such as C++ [Stroustrup 1987], C# [Hejlsberg et al. 2003b], Scala [Odersky 2014], and Haskell [Peyton Jones 2003].

Proponents of static checking argue that exceptions represent corner cases that are easy to forget. The evidence suggests they have a point. One study of a corpus of C# code [Cabral and Marques 2007b] determined that 90% of the possible exceptions are undocumented. Undocumented exceptions make it hard to know whether all exceptions are handled, and these unhandled exceptions percolate up through abstraction layers, causing unexpected software failures. Statically checked exceptions help programmers build more robust code [Venners 2003].
Opponents of static checking argue that the annotation burden of statically checked exceptions does not pay off—that statically checked exceptions are too rigid to support common design patterns and common ways in which software evolves [Black 1982; Waldhoff 2003; Eckel 2003]. They, too, have a point. The problems with statically checked exceptions have become more apparent in recent years as object-oriented (OO) languages like C#, Scala, and Java have acquired lambda expressions and the use of higher-order functions has become more common. As a result, the promise of exceptions to help make software more reliable has been partly lost.

Studies of the effectiveness of exception mechanisms have concluded that existing mechanisms do not satisfy the appropriate design criteria [Buhr and Mok 2000; Cabral and Marques 2007a]. C# does not statically check exceptions because its designers did not know how to design such an exception mechanism well, saying “more thinking is needed before we put some kind of checked exceptions mechanism in place” [Hejlsberg et al. 2003a]. It seems the long-running conflict between checked and unchecked exceptions can be resolved only by a new exception mechanism.

This paper aims to provide a better exception mechanism, one that combines the benefits of static checking with the flexibility of unchecked exceptions. The new mechanism gives programmers static, compile-time guidance to ensure exceptions are handled, but works well with higher-order functions and design patterns. It adds little programmer burden and even reduces that burden. The run-time overhead of the mechanism is low: exception handling does not require stack capture in common use cases and avoids the need to wrap checked exceptions in unchecked ones.

Two main insights underlie the new design. The first is that the distinction between “checked” and “unchecked” should not be a property of the type of the exception being raised, as it is in Java, but rather a property of the context in which the exception propagates. In contexts that are aware of an exception, the exception should be checked statically to ensure that it is handled. To handle higher-order functions and design patterns, however, some contexts must be oblivious to exceptions propagating through them; exceptions should tunnel uncaught through oblivious contexts, effectively unchecked.

This principle implies that the same exception may be both checked and unchecked at different points during its propagation. To prevent oblivious code from accidentally catching exceptions, a second insight is needed: exceptions can be distinguished by expanding the space of exception identifiers with an additional label that describes the exception-aware context in which this exception can be caught. These labels can be viewed as an extension of the notion of blame labels found in previous work on gradual typing [Wadler and Findler 2009]. Unlike with gradual typing, this sort of “blame” is not a programmer error; it is instead a way to indicate that exceptions should tunnel through the oblivious code until they arrive at the right exception-aware context.

We start the rest of the paper by exploring requirements for a good exception mechanism in Section 2. Sections 3–6 present our new exception mechanism informally in the context of a Java-like language. Section 7 defines a core language whose semantics show more precisely how the mechanism works. Using this core language, we prove the key theorem that all exceptions are handled explicitly. Section 8 describes our implementation of the new exception mechanism in the context of the Genus programming language [Zhang et al. 2015]. The effectiveness of the mechanism is evaluated in Section 9, using code drawn from real-world codebases. Related work is explored more fully in Section 10; we conclude in Section 11.

2 Design Principles for Exceptions

The goal of an exception mechanism is to simplify and regularize the handling of exceptional events, making programs more reliable. However, there are two quite different classes of exceptional events, with different design goals:
- **Failures.** Some events cannot reasonably be expected to be handled correctly by the program—especially, events that arise because of programmer mistakes. Other events such as running out of memory also fall into this category.

- **Unusual conditions.** Other events arise during correct functioning of the program, in response to an unusual but planned-for state of the environment, or even just an unusual case of an algorithm.

These two classes place different requirements on the exception mechanism. For failures, efficiency is not a concern because the program is not expected to recover. However, programmers need the ability to debug the (stopped) program to discover why the failure occurred, so it is important to collect a stack trace. Furthermore, since failures imply violation of programmer assumptions, having to declare them as part of method signatures or write handler code for them is undesirable. Nonetheless, there are cases where the ability to catch failure exceptions is useful, such as when building frameworks for executing code that might fail.

For the second class of exceptions, unusual conditions, the design goals are different. Now efficiency matters! Because exceptions are slow in many common languages, programmers have learned to avoid using them. One insight is that because unusual conditions are part of the correct functioning of the program, the overhead of collecting a stack trace is unnecessary.

Unfortunately, existing languages tend not to support the distinction between these two exception classes well. For example, typical Java usage always leads to stack-trace collection, making exceptions very expensive. At the same time, code is cluttered with handlers for impossible exceptions.

### 2.1 Higher-Order Functions and Exceptions

Current exception mechanisms do not work well in code that uses higher-order functions. An example is an ML-style `map` method that applies a function argument to each element of a list, returning a new list. Callers of the higher-order function may wish to provide as an argument a function that produces exceptions to report an unusual condition that was encountered, such as an I/O exception. Of course, we want these exceptions to be handled. But the implementation of `map` knows nothing about these exceptions, so if such exceptions do occur, they should be handled by the caller of `map`. It is unreasonable for `map` either to handle or to declare them—its code should be *oblivious* to the exceptions.

This example illustrates why otherwise statically typed functional programming languages such as ML and Haskell do not try to type-check exceptions statically [Leroy and Pessaux 2000]. The problem has also become more prominent in modern OO languages that have added *lambda expressions* and are increasingly relying on libraries that use them (e.g., JavaFX, Apache Spark). The problem is encountered even without lambda expressions, though; for example, Java’s `Iterator` interface declares no exceptions on its methods, which means that implementations of `Iterator` are not allowed to generate exceptions—unless they are made “unchecked”.

Our goal is to achieve the notational convenience of the functional programming languages along with the assurance that exceptions are handled, which is offered by languages such as Java, Swift [Swift 2014], and Modula-3 [Nelson 1991]. We propose that a higher-order function like `map` should be implementable in a way that is *oblivious* to the exceptions possibly generated by its argument. The possible exceptions of the argument should not be declared in the signature of `map`; nor should the code of `map` have to say anything about these exceptions.

A subtle problem arises when a higher-order function like `map` uses exceptions inside its own implementation. If the exceptions of the argument and the internal exceptions collide, the `map` code could then *accidentally* catch exceptions that are not intended for it—an effect we call *exception capture* by analogy with the problem of variable capture in dynamically scoped languages [Steele 1990]. For modularity, a way
is needed to tunnel such exceptions through the intermediate calling context. In fact, accidentally-caught exceptions are a real source of serious bugs [FindBugs bug descriptions; CWE].

An alternative to our oblivious-code approach that has been suggested previously [van Dooren and Steegmans 2005; Goetz 2010; Rytz et al. 2012; Leijen 2014] is to parameterize higher-order code like \texttt{map} over the unknown exceptions of its argument. This exception polymorphism approach requires writing annotations on oblivious code yet still permits accidental exception capture.

2.2 Our Approach

Backed by common sense and some empirical evidence, we believe that code is more reliable when compile-time checking guides programmers to handle exceptional cases. It is disappointing that recent language designs such as C# and Scala have backed away from statically declared exceptions.

We propose a new statically checked exception mechanism that addresses the weaknesses of prior exception mechanisms:

- It supports static, local reasoning about exceptions. Local reasoning is efficient, but more importantly, it aids programmer understanding. A code context is required to handle only the exceptions it knows about statically.

- The mechanism is cheap when it needs to be: when exceptions are used for nonlocal control flow rather than failures.

- In the failure case, however, the mechanism collects the stack trace needed for debugging.

- It supports higher-order functions whose arguments are other functions that might throw exceptions to which the higher-order code is oblivious.

- It avoids the exception-capture problem both for higher-order functions and for failures.

3 The Exception Mechanism

We use Java as a starting point for our design because it is currently the most popular language with statically checked exceptions. Our design is presented as a version of the Genus language, a variant of Java with an expressive constrained genericity mechanism [Zhang et al. 2015]. The essential ideas should apply equally well to other languages, such as Java, C# [Microsoft Corporation 2001], Scala [Odersky 2014], and ML [Milner et al. 1990]. Since exception-oblivious code (like \texttt{map}) is often generic, it is important to study how exceptions interact with sophisticated generics.\footnote{Genus uses square brackets rather than angle brackets for generic type arguments: \texttt{List[T]} rather than \texttt{List<T>}. For brevity, we use Genus syntax and the Genus equivalents of Java core classes without further explanation.}

Previous languages have either had entirely “checked” or “unchecked” exceptions (in Java’s terminology), or, as in Java, have assigned exception types to one of these two categories. Our insight is that “checked” vs. “unchecked” is a property of the context of the exception rather than of its type. Any exception should be “checked” in a context that is not oblivious to the exception and can therefore handle it. But in a context that is oblivious to the exception, the exception should be treated as “unchecked”.

Genus requires that a method handle or explicitly propagate all exceptions it knows can arise from operations it uses or methods it calls. If the implementation of a method explicitly throws an unhandled exception whose type (or the supertype thereof) is not listed in the method’s header, the program is rejected.

Like in Java, exceptions can be handled using the \texttt{try–catch} construct, and a \texttt{finally} block that is always executed may be provided. (The \texttt{try-with-resources} statement of Java 7 is easily supported; it is orthogonal to the other new features.)
A method that wishes merely to propagate an exception to its caller can simply place a throws clause in its signature. We say such an exception propagates in checked mode. Unlike in Java, exceptions in checked mode do not cause stack capture.

### 3.1 Failures

Unlike Java, our mechanism makes it easy for the programmer to indicate that an exception should not happen. The programmer ordinarily does this by putting a fails clause in the method header. Any caller of the method is then oblivious to the exception, meaning that the exception will be treated as unchecked as it propagates further. When code fails because of an exception, the exception propagates in a special mode, the failure mode.

For example, a programmer who is certain that the Object class can be loaded successfully can write

```java
Class loadObject() fails ClassNotFoundException {
    return Class.forName("genus.lang.Object");
}
```

where the method `forName` in `Class` declares `ClassNotFoundException` in its throws clause. Note that a fails clause is really part of the implementation rather than part of the method signature or specification. We write it in the header just for convenience.

Exceptions propagating in failure mode also differ in what happens at run time. Programmers need detailed information to debug the stopped program to discover how the failure occurred. Therefore, failure exceptions collect a stack trace. This is relatively slow (as slow as most Java exceptions!) but efficiency is not a concern for failures.

### 3.2 Avoiding Exception Capture

Since exceptions propagating in failure mode do not appear in method signatures, it is important to avoid catching them accidentally. For example, consider the following code that calls two functions g() and h():

```java
void f() {
    try {
        g(); // signature says "throws MyExc"
        h(); // signature doesn’t say "throws MyExc"
    } catch (MyExc e) {...}
}
```

Suppose that because of a programmer mistake, the call to h() unexpectedly fails with exception MyExc. If this exception were caught by the catch clause, f() would execute code intended to compensate for something that happened in g(). We prevent this undesirable exception capture by ensuring that failure exceptions cannot be caught by any ordinary catch clauses: failure exceptions tunnel past all ordinary catch clauses.

Although exceptions in failure mode are not normally handled, there may be value in catching them at the top level of the program or at the boundary between components, to allow for more graceful exit. Genus supports this with a rarely used catch_all construct that catches all exceptions of a given type, regardless of propagation mode. For example, if the try statement above were extended to include a second clause

```java
    } catch all (MyExc e) {...}
}
```

the first catch clause would catch the expected MyExcs thrown by g, and the second catch_all clause would catch failure-mode MyExcs tunneled through h.

### 3.3 Fail-by-Default Exceptions

Java has a commonly accepted set of exceptions that usually correspond to programmer mistakes: the built-in subclasses of RuntimeException or Error. To reduce annotation burden for the programmer, our mecha-
List[R] map[T,R](Function[T,R] f, List[T] src) {
    List[R] dest = new ArrayList[R]();
    for (T t : src) dest.add(f.apply(t));
    return dest;
}

Figure 1: A higher-order function written in Genus

List[String] x = ...; List[Class] y;
try { y = map(Class::forName, x); }
catch (ClassNotFoundException e) {...}

Figure 2: Passing a function that throws extra exceptions

nism does not ordinarily require writing a fails clause in order to convert such exceptions to failure mode. We say these exceptions fail by default.

Fail-by-default exceptions are different from Java’s unchecked exceptions. Unchecked exceptions conflate failures with ordinary exceptions that are tunneling through oblivious code but that still ought to be subject to static checking.

In contrast, fail-by-default exceptions remain in checked mode until they reach a method-call boundary; they convert from checked mode to failure mode only if the current method does not declare the exception in its throws clause. A fail-by-default exception collects a stack trace only if and when it does fail, so code can still handle exceptions like NoSuchElementException efficiently. It is therefore reasonable and useful to write code that handles such exceptions.

Genus also permits the set of fail-by-default exceptions to be changed on a per-class basis by adding a throws or fails clause to the class definition.

4 Higher-Order Abstractions and Tunneling

As discussed in Section 2.1, higher-order functions pose a problem for statically checked exception mechanisms. The same problem arises for many common object-oriented design patterns, which are essentially higher-order functions. Our solution is to tunnel exceptions through oblivious code.

For example, Genus allows the programmer to pass to the higher-order function map (Figure 1) an implementation of Function that throws exceptions, even though the signature of Function does not mention any exceptions. If the passed Function throws an exception, that exception is tunneled through the exception-oblivious code of map to the caller of the exception-aware code that called map.

In the code of Figure 2, the method forName in class Class is passed to map. This call is legal even though forName is declared to throw an exception ClassNotFoundException. Since map is oblivious to this exception, it cannot be expected to handle it. By contrast, the caller of map is aware that an object that throws exceptions is used at a type (Function) that does not declare any exceptions. Because it is aware of the exception, the caller is responsible for the exception.

If ClassNotFoundException arises at run time, it tunnels through the code of map and is caught by the catch clause. Alternatively, the caller could have explicitly converted the exception to a failure (via a fails clause) or explicitly allowed it to propagate (via a throws clause). In any case, exception handling is enforced statically.
interface Visitor {
    void visit(IfTree t);
    ...
}

class IfTree implements Tree {
    void accept(Visitor v)
    {
        v.visit(this);
    }
    ...
}

class Pretty implements Visitor {
    void visit(IfTree t) {
        try {
            // pretty-print IfTree
            catch (IOException e) {
                throw new UncheckedIO(e);
            }
        } // wraps IOException
    }
    void printTree(Tree t, Pretty v) throws IOException {
        try {
            t.accept(v);
        } catch (UncheckedIO u) {
            throw u.getCause();
        }
    } // unwraps UncheckedIO

class UncheckedIO extends RuntimeException {...}

Figure 3: The pretty-printing visitor in javac (simplified). Code for exception wrapping and unwrapping is highlighted.

weak interface Visitor{
    void visit(IfTree t);
    ...
}

class IfTree implements Tree {
    void accept(Visitor v) {
        v.visit(this);
    }
    ...
}

class Pretty implements Visitor {
    void visit(IfTree t) throws IOException {
        try {
            t.accept(v);
        } catch (UncheckedIO u) {
            throw u.getCause();
        }
    } // unwraps UncheckedIO

class UncheckedIO extends RuntimeException {...}

Figure 4: Exception tunneling in javac, ported to Genus.

4.1 Exception Tunneling is Safe and Light

In Java, the rigidity of checked exceptions has led to some verbose and dangerous idioms, especially when higher-order functions and design patterns are used. Exception tunneling helps avoid these undesirable programming practices.

In particular, Java programmers often abandon static checking of exceptions to make it possible for their exceptions to pass through exception-oblivious higher-order code. They either define their own exceptions as unchecked, or they cope with preexisting checked exceptions by calling unsafe APIs like sun.misc.Unsafe::throwException [Mastrangelo et al. 2015], or by wrapping checked-exception objects inside unchecked-exception objects. Wrapping with unchecked exceptions is the safest of these workarounds because it makes exception capture less likely, but wrappers are verbose and expensive.

Figure 3 shows an example of this idiom taken from the javac compiler [OpenJDK javac], which contains a number of visitors for the Java AST. In order to conform to the Visitor interface, the visit methods in the pretty-printing visitor (Pretty) wrap the checked IOException into unchecked wrappers, which are then unwrapped as shown in method printTree. This programming pattern is verbose, abandons static checking, and is likely to be slow due to stack capture.

When written in Genus, the same visitor pattern (Figure 4) does not require exception wrapping or unwrapping to achieve tunneling. The modifier weak on the interface Visitor (see Section 4.4) makes it legal for its implementations to declare new exceptions (the interface Function is annotated similarly). In printTree, the call t.accept(v) passes a visitor object that throws the additional exception IOException.
4.2 Tunneling Checked Exceptions

Earlier we discussed two modes of exception propagation: checked mode and failure mode. Tunneling mode is a third mode of propagation. The relationships between the three modes are summarized in Figure 5. In tunneling mode, as in checked mode, static checking enforces handling of exceptions. As in failure mode, these exceptions do not need to be declared in signatures of the methods they tunnel through.

A given exception may propagate in more than one mode. Consider the alternative, slightly contrived implementation of map in Figure 6. It calls a helper method mapImpl, which then recursively calls itself to traverse the list. Suppose an exception arises when function \( f \) is applied to the sixth element in the list. Figure 6 shows a snapshot of the current call stack. Since \( f \) is the place where the exception is generated, the exception first propagates in checked mode within the function \( f \). Because its caller mapImpl is oblivious to the exception, the exception then switches to tunneling mode and propagates through all the mapImpl stack frames. Finally, the caller of map knows about the exception and thus can handle it. The exception returns to checked mode when it reaches this caller. From there, it can be either caught, rethrown in checked mode, or turned into failure.

4.3 Tunneling, Exception Capture, and Blame

Tunneling avoids the phenomenon of exception capture discussed in Section 3. In OO languages like Java and C#, exception capture occurs because of an unexpected collision in the space of exception identifiers;
an exception identifier in these languages is simply the exception type. We avoid exception capture by augmenting the identity of a thrown exception to include a notion of “blame”.

To ensure that every exception is eventually either handled or treated as a failure, a method must discharge every exception it is aware of statically. There are three ways to discharge an exception: 1) handle it with a catch clause, 2) propagate it to its caller as a checked exception via a throws clause, or 3) convert it to a failure via a fails clause (which is implicit for fail-by-default exceptions).

Each of these three ways discharges exceptions from a set of program points that are statically known to give rise to these exceptions. We say these program points can be blamed for the exception. With each such program point, we associate a blame label that identifies where responsibility lies for the exception.

At run time, then, a thrown exception is identified both by its exception type, and by its blame label. An exception is discharged (e.g., caught by a catch clause, or converted to failure by a fails clause), only if the blame label of the exception lies within the lexical scope covered by that particular discharging point. Otherwise, the exception is one that the discharging point is oblivious to.

We use the word “blame” because this mechanism is related to the notion of blame used in work on behavioral contracts [Findler et al. 2001; Findler and Felleisen 2002] and gradual typing [Wadler and Findler 2009]. A compiler for a gradually typed language might label program points with unique identifiers wherever there is a mismatch between expected and actual types. When a cast failure happens at run time, blame can be attributed to the program point at fault.

Here, mismatch occurs analogously when the type of an actual argument declares exceptions not encompassed by those declared by the formal parameter type. Any exception mismatch in the parameters passed to a method call causes blame to be assigned to the program point of the method call. However, unlike in gradual typing, exceptions arising from a program point assigned blame do not imply mistakes, since the programmer must discharge the exceptions.

For example, in Figure 2, the program point where Class::forName is used at type Function is in the scope of the ensuing catch clause at line 3. Because it creates a mismatch with the signature of Function, this program point can be blamed for the exception. Similarly, in Figure 4, the shaded program point (line 2) where a Pretty object is used at type Visitor is in the scope of the clause throws IOException (line 1). Because there is a mismatch between Pretty and Visitor, the shaded program point can be blamed for the exception. Throughout the paper, we highlight program points that are assigned blame and their matching discharging points.

4.4 Weak Types

Some supertypes, usually interfaces, abstract across families of otherwise unrelated subtypes. Such interfaces often arise with design patterns like Iterator and Visitor. The intention of such types is to capture only a fragment of the behavior—a core set of methods—so that various implementations can have a common interface other software components can use.

Frequently there is utility in allowing subtypes of these interfaces to throw new exceptions. For example, suppose a lexer breaks input files into tokens; an Iterator might be used to deliver the tokens to code that consumes them. However, reading from a file can cause an IOException; the exception cannot reasonably be handled by the iterator, so should be propagated to the client code. In Java, programmers cannot throw a checked exception like IOException in such an implementation; they must either resort to unchecked exceptions, abandoning static checking, or define their own interfaces that compose poorly with existing components.

Genus addresses this need for flexibility. Methods that allow their overridings to throw new exceptions are declared with the weak modifier. The weak modifier can also be applied to a type definition to con-
weak interface Iterator[E] {
    E next() throws NoSuchElementException;
    // The exception indicates iteration is over
    ...
}  

class Tokenizer implements Iterator[Token] {
    Token next() throws IOException, NoSuchElementException {...}
    ...
}

Figure 7: The Iterator interface and an inexact subtype

Iterator[Token] iter = new Tokenizer(reader);
while (true) {
    Token t;
    try { t = iter.next(); }
    catch (NoSuchElementException e) { break; }
    catch (IOException e) { log.write(...); continue; }
    ...
}

Figure 8: Using a Tokenizer as an Iterator generates blame.

veniently indicate that all methods in that type are intended to be weak; see the definition of Iterator in Figure 7 for an example.

A subtype of a weak type can be inexact; for example, the Tokenizer class in Figure 7 is inexact with respect to its weak interface since its next method adds IOException. A Tokenizer can be used as an Iterator but this generates blame, forcing IOException to be handled, as in Figure 8.

**Behavioral subtyping and conformance.** Behavioral subtyping [Liskov and Wing 1994] is based on the idea that the allowed uses of an object should be known based on its apparent type. Therefore, an overriding method cannot add new exceptions to the supertype’s signature for the method.

Our mechanism relaxes this requirement for weak types. Methods of an inexact subtype must obey the supertype specification—except that they can throw more exceptions. This implies that their additional exceptional conditions must be signaled with different types than those in the supertype method—Tokenizer indicates an I/O problem by throwing IOException, not NoSuchElementException—and that the exceptional conditions the supertype defines must not be signaled in other ways—Tokenizer cannot issue a failure or return null when the iteration has no more elements.

5 Generics and Exceptions

We have also used Genus to explore the important interaction between exceptions and mechanisms for constrained parametric polymorphism. Various languages constrain generic type arguments in various ways: for example, Java and C# use subtyping constraints, whereas Haskell and Genus use the more flexible mechanism of type classes [Wadler and Blott 1989].

Genus provides constrained parametric polymorphism via constraints and models [Zhang et al. 2015]. Like type classes, Genus constraints are predicates describing type features required by generic code. Genus models show how types can satisfy constraints, like type class instances in Haskell. Unlike Haskell instances, models are explicitly part of the instantiation of a generic abstraction. For example, the two instantiations Set[String] and Set[String with CaseInsensEq] are different types distinguished by the use of the
class ObjectPool<T> {
    Factory<T> f;
    T borrow() throws Exception
        {... f.make() ...}
    ...
}

interface Factory<T> {
    T make() throws Exception;
}

class ConnFactory implements Factory<Connection> {
    Factory<Connection> make()
        throws SQLException {...}
}

6 Exactness Analysis

The new exception mechanism poses new challenges for type checking. One challenge is that the identity of an exception includes a blame label, so blame should not be allowed to escape its scope. Otherwise, an exception might not be handled.

For example, consider the first definition of the PeekingIterator class in Figure 10. It decorates a wrapped Iterator in field inner to support one-element lookahead. Its next and peek methods call inner.next(). Per Section 4.4, it is possible to pass an object of some inexact subtype of Iterator to the constructor, to be assigned to inner. However, Iterator is a weak type, so the methods of the actual
class PeekingIterator[E] implements Iterator[E] {
    Iterator[E] inner;
    PeekingIterator(Iterator[E] it) { inner = it; ...}
    E peek() throws NoSuchElementException
    { ... inner.next() ...}
    ...
}

class PeekingIterator[I extends Iterator[E], E] implements Iterator[E] {
    I inner;
    PeekingIterator(I it) { inner = it; ...}
    E peek() throws NoSuchElementException
    { ... inner.next() ...}
    ...
}

Figure 10: Two definitions of `PeekingIterator`. The top one allows blame to escape, but a warning is issued for the constructor. The bottom one uses dependent exactness to soundly avoid the warning.

An object being passed may throw exceptions not declared by `Iterator`. If the assignment to `inner` were allowed, the same exceptions would propagate when the `next` method of the `PeekingIterator` object were called. And this call could be delayed until outside the context that is aware of the mismatch with `Iterator`. In this case, the exceptions would not be guaranteed to be handled.

Therefore, we want to detect statically that the assignment to `inner` lets the blame from the inexact object escape. Storing an inexact object into a data structure at a weak type, or even returning an inexact object from a method, may permit such an escape of blame.

A second challenge for the new exception mechanism, and indeed for exception mechanisms generally, is that programmers should not be forced to write handlers for program points where exceptions cannot happen. To address this challenge, the location of blame should be precise. Figure 8 offers an example of this problem. The method call `iter.next()` might appear (to the compiler) not to throw any exceptions because `iter` has type `Iterator<Token>`, yet we know that it may throw an `IOException` because `iter` is initialized to a `Tokenizer`. A safe, conservative solution would be to require all of the code below this initialization to be wrapped in a `try–catch`. But this solution would make it difficult to continue the iteration after an `IOException` is raised.

Genus addresses these two challenges using an intraprocedural program analysis that assigns exactness to uses of weak types, with little annotation effort by the programmer.

### 6.1 Exactness Annotations and Exactness Defaults

**Indicating intolerance of inexactness at use sites.** When a formal parameter or local variable is assigned a weak type, the programmer can annotate the type with `@exact` to indicate that an exact subtype must be used. For example, if the programmer adds `@exact` to the formal parameter of the constructor at line 3 in Figure 10,

```java
PeekingIterator(@exact Iterator[E] it) {inner = it;...}
```

it becomes a static error to pass an inexact implementation of `Iterator` to the constructor. So it is guaranteed that using `inner` will not generate unexpected exceptions. By contrast, without `@exact`, Genus issues a warning about the assignment to the escaping pointer `inner` at line 3. If the exception is actually thrown at run time, it is converted into failure and the usual stack trace is captured.

Although `@exact` might appear to add notational burden, our experience with porting existing Java code into Genus (Section 9) suggests that this escape hatch is rarely needed. We have not seen the need
to use the @exact annotation to dismiss such warnings in existing code ported from Java. It seems that
programmers use weak types differently from other types—weak types provide functionality rather than
structure. Further, exactness defaults and exactness inference (Section 6.2) reduce annotation overhead, and
exactness-dependent types (Section 6.3) provide more expressiveness.

**Exactness defaults.** Exactness defines what exceptions that are not declared by the weak type might nev-
ertheless be generated by the term being typed. Exactness $E$ is formally a mapping from methods to sets of
exceptions. These mappings form a lattice ordered as follows:

$$E_1 \leq E_2 \iff \text{dom}(E_1) \subseteq \text{dom}(E_2) \land \forall m. E_1(m) \subseteq E_2(m)$$

The bottom lattice element is strict exactness, denoted by $\emptyset$.

To avoid the need for programmers to write the annotation @exact for most uses of weak types, the
compiler determines exactness using a combination of exactness defaults and automatic exactness inference.
To see how these mechanisms work, consider the code in Figure 11.

1. Weak types used as return types or field types are exact, as these are the channels through which
pointers can escape. For these types, we have $E = \emptyset$.

2. Methods and constructors are implicitly polymorphic with respect to exactness. That is, they can be
viewed as parameterized by the exactness of their argument and receiver types.

3. Weak types in a local context are labeled by exactness variables: for example, $x$ and $y$ in Figure 11,
at lines 2 and 11 respectively.

   A unification-based inference engine solves for these variables, inferring exactness from the local
variable uses (Section 6.2).

4. For a procedure call, an exactness variable is generated for each argument and/or receiver whose
formal parameter type is weak. Exactness variables of this kind in Figure 11 are $z$ (line 9) and $w$
(line 12).

5. Recall that Genus supports constrained parametric polymorphism via type constraints [Zhang et al.
2015]. Subtype constraints and where-clause constraints can also specify exactness. Their default
exactness is deduced in ways similar to those listed above. For example, in Figure 11 the use of
Runnable in g’s signature (line 1) constrains the type parameter $T$, so its exactness is resolved to a
fresh name $e$, with respect to which $g$ is polymorphic.

### 6.2 Solving Exactness Constraints

At each assignment (including variable initialization and argument passing) to a variable with weak type $\tau$,
inexact values must not escape into variables with exact types. Therefore, constraints of form $\tau(E_r) \leq \tau(E_l)$
are generated, where $E_l$ is the exactness of the left-hand side expected type $\tau$ in an assignment, resolved as
described in Section 6.1, and $E_r$ is the exactness of the right-hand side actual type with respect to $\tau$. For
example, the code of Figure 11 then generates the following constraints with line numbers attached:

\[
\begin{align*}
\tau(E_r) & \leq \tau(E_l) \\
\text{Runnable} \{\{\text{run} \mapsto \text{IOException}\}\} & \leq \text{Runnable}(x) \quad 4 \\
\text{Runnable} \{\{\text{run} \mapsto \text{EOFException}\}\} & \leq \text{Runnable}(x) \quad 7 \\
\text{Runnable}(x) & \leq \text{Runnable}(z) \quad 9 \\
\text{Runnable}(e) & \leq \text{Runnable}(y) \quad 11 \\
\text{Runnable}(y) & \leq \text{Runnable}(w) \quad 12 \\
\text{Iterator}[T](\emptyset) & \leq \text{Iterator}[T](e) \quad 11
\end{align*}
\]
Figure 11: Running example for exactness analysis. Uses of weak types are tagged by exactness variables, to be fed into the solver. (EOFException is a subtype of IOException.)

The last constraint is due to desugaring of the loop at lines 11–12:

```java
for (Iterator[T]⟨v⟩ i = l.iterator();;) {
    Runnable⟨y⟩ r;
    try { r = i.next(); }
    catch (NoSuchElementException ex) { break; }
    r.run();
}
```

Note that enhanced for loops are translated differently by Java and Genus. Genus exceptions are fast enough that it is often faster to call next() and catch a final exception, rather than calling hasNext() on every iteration.

The compiler solves these constraints by finding the least upper bounds of \(x, y, z, w,\) and \(v\):

\[
x = z = \{ \text{run} \mapsto \{ \text{IOException}, \text{EOFException} \} \}
\]
\[
y = w = e
\]
\[
v = \emptyset
\]

The fact that a solution exists implies that inexact pointers will not escape to the heap, addressing the first challenge of escaping blame.

The solution also reveals precisely where exception handling is required, addressing the second challenge of blame precision. Specifically, the solution to each variable generated via the fourth case of exactness defaults (Section 6.1) tells what exception can be produced by the method call. In our running example, the solution to \(z\) is that the method call \(r_0.run()\) may throw IOException or EOFException, which are handled by the catch block. Notice that although mismatches happen at lines 4 and 7, the blame does not take effect until the method call at line 9.

The solution to \(w\) is the polymorphic label \(e\), which means that the current context is oblivious to whatever exceptions correspond to \(e\) when \(g\) is called, as discussed in Section 4.

### 6.3 Exactness-Dependent Types

It is possible to write a type-safe PeekingIterator using the @exact annotation, but we might want a peeking iterator that throws the same exceptions as its underlying iterator does. This expressiveness can be obtained by making PeekingIterator talk about the potential mismatch, as in the bottom definition of PeekingIterator in Figure 10. The class is now parameterized by the type of the iterator itDecorates. In
the using code below, PeekingIterator is instantiated on an inexact subtype of Iterator, so the compiler requires the exception to be handled:

```java
try {
    PeekingIterator[Tokenizer, Token] pi =
    new PeekingIterator[Tokenizer, Token](...);
    while (pi.hasNext()) {... pi.peek() ...}
} catch (IOException e) {...}
```

Parameterized by a weak constraint, the Genus version of the `ObjectPool` type in Figure 9 is similarly exactness-dependent.

The special `this` variable, when referring to the current object of a weak class, also has an exactness-dependent type—it is dependent on the exactness of the run-time class of the object with respect to the enclosing weak class. Since the run-time class is statically unknown, the compiler must assume that it can add arbitrary exceptions. Thus it is a static error to use the receiver `this` in ways that generate blame. We do not expect this rule to limit expressiveness much: most weak types are interfaces, which do not normally use this.

7 Formalization

We formalize the new exception mechanism using a core calculus, CBC (for Checked Blame Calculus).

7.1 Syntax and Notations

Figure 12 defines both a surface and a kernel syntax for CBC. Programs are written in the surface syntax, and rewritten to and evaluated in the kernel calculus. Applications in surface terms are tagged by unique blame labels (ranged over by \( \ell \)) representing lexical positions where blame can arise. Rewriting propagates these labels from the surface language to the kernel language, for blame tracking during kernel evaluation.

The surface syntax assumes a fixed set of exception names ranged over by \( E \). The kernel syntax allows them to be labeled to form new names; \( E \) and \( E^\ell \) are different names.

Surface types (\( \tau \)) include weak types and strong types. A strong type (\( \sigma \)) is either the base type \( B \) or a function type \( \tau \rightarrow [\sigma]_E \) that does not allow mismatch against \( E \). (An overline denotes a (possibly empty) set.) A weak type \( \tau \rightarrow [\sigma]_E \), on the other hand, tolerates mismatch. Notice that function return types must be strong to prevent blame from escaping. The same can be said about kernel types. Since there is an obvious injection (syntactic identity) from surface types to kernel types, we abuse notation by using \( \tau \) and \( \sigma \) in places where kernel types \( T \) and \( S \) are expected.

Environments \( \Gamma \) contain mappings from variables to their types and exactness. Exactness is represented by sets of exceptions. Strong types enforce strict exactness, so their exactness is represented by \( \emptyset \). The auxiliary function \( K(\cdot) \) returns \( \bot \) for strong types and \( \top \) for weak types; values of strong types must not escape. \( \Gamma_\bot \) retains only the strongly-typed variables in \( \Gamma \).

7.2 Semantics

Surface-to-kernel rewriting. Figure 13 defines the rewriting rules. The judgment \( \Gamma; K \vdash f \rightsquigarrow e : [\tau]_E \) translates the surface term \( f \) to the kernel term \( e \), assigns \( f \) the type \( \tau \), and infers the exceptions \( E \) that evaluating \( e \) might raise.

Typing is dependent on \( K \), which indicates whether the term in question is guaranteed not to escape. For example, the left-hand-side term in an application is type-checked with \( K = \top \) as in R-APP-E and R-APP-I, while the body of an abstraction is type-checked with \( K = \bot \) as in R-ABS. R-VAR-W denies
first-class citizenship to weakly typed variables, and augments the return type if the environment indicates inexactness.

Exception mismatch is computed using the subtyping relation $\preceq$, as in R-APP-I and R-LET. But only with R-APP-I can blame take effect, and its translation is consequently less obvious. To avoid exception capture, we need to give new names to exceptions involved in the mismatch. Therefore, the translation wraps the argument in an abstraction, which, when applied, catches any exceptions in the mismatch ($E$) and rethrows their labeled versions ($E\ell$). The caller is aware of the exceptions $E$, so it catches the labeled exceptions tunneled to its context and strips off their labels.

**Semantics of the kernel calculus.** Figure 14 defines the static semantics of the kernel, and Figure 15 gives the dynamic semantics. The static semantics is largely similar to the typing induced by rewriting, except that the kernel need not worry about exception capture. Hence, exception propagation happens in the usual way.

### 7.3 Type Safety

The type system guarantees that if a program can be typed without exceptional effects, it cannot get stuck when evaluated, or terminate in an exception. This guarantee easily follows from two other standard results.

First of all, the kernel type system is sound:

**Theorem 1 (Kernel soundness: preservation and progress)**

- If $\emptyset; K \vdash e : [T]_{\Gamma}$ and $e \longrightarrow e'$ then $\emptyset; K \vdash e' : [T]_{\Gamma}$.
- If $\emptyset; K \vdash e : [T]_{\Gamma}$ then either
  1. $\exists v. e = v$, or
  2. $\exists U_0 \in \Upsilon. e = \text{throw } U_0$, or
  3. $\exists e'. e \longrightarrow e'$.
\[
\Gamma; K \vdash f \leadsto e : [\tau]_{E_1}^E
\]

[R-CONST] \[
\Gamma; K \vdash b \leadsto b : [B]_{\emptyset}
\]

[R-VAR-S] \[
x : \sigma(\emptyset) \in \Gamma_K 
\Gamma; K \vdash x \leadsto x : [\sigma]_{\emptyset}
\]

[R-VAR-W] \[
x : \tau \vdash \sigma \cap E_1 \cap E_2 \in \Gamma_K 
\Gamma; K \vdash x \leadsto x : [\tau \vdash \sigma | E_1 \cup E_2]_{\emptyset}
\]

[R-ABS] \[
\Gamma_K, x : \tau(\emptyset); \bot \vdash f \leadsto e : [\sigma]_{E_1}^E 
\Gamma; K \vdash \lambda x : \tau . f \leadsto \lambda x : \tau . e : [\tau \vdash \sigma]_{E_1}^E
\]

[R-LET] \[
\Gamma; K \vdash f_1 \leadsto e_1 : [\tau_1]_{E_1}^E \quad \tau_3 \subseteq E_1 \quad \tau_1, \tau_2 : \tau_1_1(\emptyset); K \vdash f_2 \leadsto e_2 : [\tau_2]_{E_1}^E 
\Gamma; K \vdash f_1 f_2 \leadsto e_1 e_2 : [\sigma]_{E_1 \cup E_2 \cup E_3}^E
\]

[R-APP-E] \[
\Gamma; K \vdash f_1 f_2 \leadsto e_1 e_2 : [\sigma]_{E_1 \cup E_2 \cup E_3}^E 
\Gamma; K \vdash f_1 \leadsto e_1 : [\tau_1]_{E_1}^E \quad \Gamma; K \vdash f_2 \leadsto e_2 : [\tau_2]_{E_2}^E \quad \tau_2 \subseteq \emptyset \quad \tau_1 \quad \tau_2 \subseteq \emptyset \quad \tau_1
\]

[R-APP-I] \[
\Gamma; K \vdash \{ f_1 f_2 \} \leadsto \text{try } e_1 \left(\text{let } x : \tau_2 \leftarrow e_2 \text{ in } \lambda y : \tau_1 \cdot \text{try } x : e \text{ catch } E \vdash \text{throw } E'\right) \text{ catch } E' \vdash \text{throw } E : [\sigma]_{E_1 \cup E_2 \cup E_3 \cup E_4}^E
\]

[R-TRY-CATCH] \[
\Gamma; K \vdash f_1 \leadsto e_1 : [\tau]_{E_1}^E \quad \Gamma; K \vdash f_2 \leadsto e_2 : [\tau]_{E_2}^E \quad E \in E_1 
\Gamma; K \vdash \text{try } f_1 \text{ catch } E \vdash f_2 \leadsto e_1 \text{ catch } E \vdash e_2 : [\tau]_{E_1 \cup E_2}^E
\]

[R-THROW] \[
\Gamma; K \vdash \text{throw } E \leadsto \text{throw } E : [\sigma]_{E_1}^E
\]

[R-SUBSUME] \[
\Gamma; K \vdash f \leadsto e : [\tau_1]_{E_1}^E \quad \tau_1 \subseteq \emptyset \quad \tau_2 \quad \tau_1 \subseteq \tau_2 \quad E_1 \subseteq E_2 
\Gamma; K \vdash f \leadsto e : [\tau_2]_{E_2}^E
\]

[SS-B] \[
B \subseteq \emptyset \quad B
\]

[SS-S] \[
\tau_2 \subseteq \emptyset \quad \tau_1 \subseteq \emptyset \quad \sigma_1 \subseteq \emptyset \quad \sigma_2 
\tau_1 \vdash \sigma_1 | E_1 \subseteq E_2 \quad \tau_2 \vdash \sigma_2 | E_2
\]

[SS-W] \[
\tau_2 \subseteq \emptyset \quad \sigma_1 \subseteq \emptyset \quad \sigma_2 
\tau_1 \vdash \sigma_1 | E_1 \subseteq E_1 \cup E_2 \quad \tau_2 \vdash \sigma_2 | E_2
\]

---

Figure 13: Surface-to-kernel rewriting
\[
\Delta; K \vdash e : [T]_{U}
\]

[T-SUBSUME] \[
\Delta; K \vdash e : [T_1]_{U_1} \quad T_1 \subseteq \emptyset \quad T_2 \quad U_1 \subseteq U_2
\]
\[
\Delta; K \vdash e : [T_2]_{U_2}
\]

[T-CONST] \[
\Delta; K \vdash b : [B]_{\emptyset}
\]

[T-VAR-S] \[
x : S(\emptyset) \in \Delta_K
\]
\[
\Delta; K \vdash x : [S]_{\emptyset}
\]

[T-VAR-W] \[
x : T \xrightarrow{\tau} [S]_{U_2}(U_2) \in \Delta_K
\]
\[
\Delta; K \vdash x : [T \xrightarrow{\tau} [S]_{U_1 \cup U_2}]_{\emptyset}
\]

[T-ABS] \[
\Delta_K, x : T(\emptyset) ; \perp \vdash e : [S]_{U}
\]
\[
\Delta; K \vdash \lambda x : T. e : [T \xrightarrow{\tau} [S]_{U}]_{\emptyset}
\]

[T-APP] \[
\Delta; T \vdash e_1 : [T_1 \xrightarrow{\tau} [S]_{U_1}]_{U_1}
\]
\[
\Delta; K \vdash e_2 : [T_2]_{U_2}
\]
\[
T_2 \subseteq U_1
\]
\[
\Delta; K \vdash e_1 e_2 : [T]_{U_1 \cup U_2 \cup U_3 \cup U}
\]
\[
\Delta; K \vdash e_1 e_2 : [T]_{U_1 \cup U_2 \cup U_3 \cup U}
\]

[T-LET] \[
\Delta; K \vdash e_1 : [T_1 \xrightarrow{\tau} [S]_{U_1}]_{U_1}
\]
\[
\Delta; K \vdash e_2 : [T_2]_{U_2}
\]
\[
T_2 \subseteq U_1
\]
\[
\Delta; K \vdash \lambda x : T. e_1 \in e_2 : [T_2]_{U_1 \cup U_2}
\]
\[
\Delta; K \vdash \lambda x : T. e_1 \in e_2 : [T_2]_{U_1 \cup U_2}
\]

[T-THROW] \[
\Delta; K \vdash \text{throw} U : [S]_{U}
\]

[T-TRY-CATCH] \[
\Delta; K \vdash e_1 : [T]_{U_1}
\]
\[
\Delta; K \vdash e_2 : [T]_{U_2}
\]
\[
U \subseteq U_1
\]
\[
\Delta; K \vdash \text{try } e_1 \\text{catch } U \uparrow e_2 : [T]_{(U \uparrow U) \cup U_2}
\]
\[
\Delta; K \vdash \text{try } e_1 \\text{catch } U \uparrow e_2 : [T]_{(U \uparrow U) \cup U_2}
\]

[KS-B] \[
B \subseteq \emptyset \quad B
\]

[KS-SS] \[
T_2 \subseteq \emptyset \quad T_1 \quad S_1 \subseteq \emptyset \quad S_2 \quad U_1 \subseteq U_2
\]
\[
T_1 \xrightarrow{\tau} [S_1]_{U_1} \subseteq \emptyset \quad T_2 \xrightarrow{\tau} [S_2]_{U_2}
\]

[KS-*W] \[
T_2 \subseteq \emptyset \quad T_1 \quad S_1 \subseteq \emptyset \quad S_2
\]
\[
T_1 \xrightarrow{\tau} [S_1]_{U_1} \subseteq \emptyset \quad T_2 \xrightarrow{\tau} [S_2]_{U_2}
\]

Figure 14: Static semantics of the kernel
Values
\[ v ::= k \mid \lambda x:T.e \]

Evaluation contexts
\[ C ::= \emptyset \mid C.e \mid v.C \mid \text{let } x:T \leftarrow C \text{ in } e \mid \text{try } C \text{ catch } U \triangleright e \]

**Figure 15:** Dynamic semantics of the kernel

- **[Beta]**
  \[ (\lambda x:T.e) v \rightarrow e[v/x] \]

- **[Let]**
  \[ \text{let } x:T \leftarrow v \text{ in } e \rightarrow e[v/x] \]

- **[Try]**
  \[ \text{try } v \text{ catch } U \triangleright e \rightarrow v \]

- **[Catch]**
  \[ \text{try } (\text{throw } U) \text{ catch } \ldots U \triangleright e \ldots \rightarrow e \]

- **[Throw]**
  \[ \text{throw } U \leftarrow C \]

- **[Context]**
  \[ e \rightarrow e' \]

\[ C[e] \rightarrow C[e'] \]

\[ \text{throw } U \leftarrow C \]

\[ \text{throw } U \rightarrow \emptyset \]

\[ \text{throw } U \rightarrow v \]

\[ \text{throw } U \rightarrow \text{let } x:T \leftarrow \emptyset \text{ in } e \]

\[ \text{throw } U _0 \rightarrow \text{try } \emptyset \text{ catch } U \triangleright e \ (U_0 \notin U) \]

**Proof.** This is proved in the usual way, by induction on the kernel typing derivation. See the appendix for details of this proof and of other formal results in this paper.

Second, the translation from the surface language to the kernel language is type-preserving:

**Lemma 1 (Rewriting preserves types)** If \( \Gamma;K \vdash f \rightsquigarrow e : [\tau]_E \) then \( \Gamma;K \vdash e : [\tau]_E \).

**Proof.** By induction on the derivation of the translation.

The guarantee that well-typed programs handle their exceptions is a direct corollary of these two previous results:

**Corollary 1 (No uncaught exceptions)** If \( \emptyset;\bot \vdash f \rightsquigarrow e : [\tau]_E \) then \( \exists v. e \rightarrow^* v \).

## 8 Implementation

We have implemented the new exception mechanism for the Genus programming language. The implementation consists of about 5,800 lines of code, extending the compiler for the base Genus language [Zhang et al. 2015]. Genus is implemented using Polyglot [Nystrom et al. 2003], so code generation works by translating to Java code, using a Java compiler as a back end.

The rest of this section focuses on the translation into Java. The translation is guided by two goals: 1) it should prevent accidental capturing of exceptions, and 2) it should add negligible performance overhead to normal control flow.

### 8.1 Representing Non-Checked Exceptions

Unlike exceptions in checked mode, exceptions traveling in tunneling mode or failure mode must acquire new identities to avoid accidental capturing. These identities are implemented by wrapping exceptions into
class Blame extends RuntimeException {
    Throwable inner;
    Blame(Throwable t) { inner = t; }
    Throwable fillInStackTrace() { return this; }
} // represents exceptions in tunneling mode

class Failure extends RuntimeException {
    Throwable inner;
    Failure(Throwable t) { inner = t; }
} // represents exceptions in failure mode

Figure 16: The Blame and Failure classes in the Genus runtime

objects of classes Blame and Failure (Figure 16). Both classes extend RuntimeException, but Blame does not collect a stack trace.

8.2 Translating Exception-Oblivious Code

Methods with weakly typed parameters ignore extra exceptions generated by them. To ensure they are handled in the appropriate context, weakly typed parameters, including the receiver, are accompanied by an additional Blame argument that serves as the blame label. When the actual argument is exact, the Blame argument is null. For example, the weak type Iterator has the following translation:

interface Iterator<E> {
    E next$Iterator(Blame b$) throws NoSuchElementException;
    ...
}

It receives a Blame object from its caller to accompany the weakly typed receiver. If an implementation of Iterator throws a mismatched exception, it is wrapped in this Blame object and tunneled through the code oblivious to it.

Exception-oblivious procedures are translated in a similar way. For example, the code generated for map (Figure 1) looks like the following:

<T,R> List<R> map(Function<T,R> f, List<T> s, Blame b$) {
    ... f.apply$Function(t, b$) ... }

The extra Blame argument b$ is intended for potential mismatch in the argument function f, and is passed down to the method call f.apply$Function(...) so that exceptions from f have the right blame label.

8.3 Translating Exception-Aware Code

The definition of Iterator’s inexact subtype Tokenizer is exception-aware. Its translation is shown in the top of Figure 17. Per Java’s type-checking rules, the overriding method in Tokenizer cannot throw extra checked exceptions. Instead, the overriding method next$Iterator(Blame) redirects to method next() that does the real work, possibly throwing an IOException, and then turns that exception into either a Blame or a Failure, which is unchecked. If the Blame argument is not null, there must be a program point ready to handle the exception. So the IOException is wrapped in the Blame object and is tunneled to that program point. If the Blame object is null, a Failure object wrapping the IOException is created and thrown. This might happen, for example, if the programmer chose to disregard the compiler warning reported for passing a Tokenizer (Figure 7) into the constructor of PeekingIterator (top of Figure 10).

The code in Figure 8 is also exception-aware, and Figure 17 (bottom) shows its translation. Instead of creating a new Blame object every time a mismatch happens, each thread maintains a Blame object pool that recycles Blame objects. A Blame object is borrowed from the pool at the blamable program point in the try block, and is returned in the finally block. The catch block catches any Blame, but only executes the
class Tokenizer implements Iterator<Token> {
    Token next$Iterator(Blame b$) throws NoSuchElementException {
        try { return next(); }
        catch (IOException e) {
            if (b$ != null) { b$.inner = e; throw b$; }
            else throw new Failure(e);
        }
    }
    Token next() throws IOException, NoSuchElementException {...}
    ...
}

Blame b$ = null;
try {
    Iterator<Token> iter = new Tokenizer(reader);
    while (true) {
        Token t;
        try { t = iter.next$Iterator(b$=Thread.borrowB$()); }
        catch (NoSuchElementException e) { break; }
        catch (Blame bCaught$) {
            if (bCaught$ == b$) { log.write(...); continue; }
            else throw bCaught$;
        }
    }
} finally { Thread.handbackB$(b$); }

Figure 17: Translating exception-aware code (Tokenizer from Figure 7 and its using code from Figure 8) into Java

Aggressive interweaving of try–catch in method bodies might preclude certain compiler optimizations. Therefore, the translation uses a simple program analysis to identify existing enclosing try blocks onto which these new catch blocks can be attached.

8.4 Translating Failure Exceptions

A method body is wrapped in a try block whose corresponding catch block catches all exceptions that will switch to failure mode after exiting the method. A catch all block is translated into possibly multiple catch blocks to also catch compatible Failure and Blame objects.

9 Evaluation

The aim of our evaluation is to explore the expressiveness of the new exception mechanism, and its overhead with respect to both performance and notational burden.

9.1 Porting Java Code to Use Genus Exceptions

To evaluate the expressive power of the new exception mechanism, we ported various existing Java programs and libraries into Genus. Some of this code (ObjectPool and PeekingIterator) is described earlier, but we examined some larger code samples:
• We ported the Java Collections Framework and found that no \texttt{@exact} annotations were needed. In addition, the Genus compiler found unreachable code in \texttt{AbstractSequentialList}, thanks to fail-by-default exceptions propagating in checked mode (Section 3.3).

• We ported the \texttt{javac} visitor of Figure 3 into Genus, as mentioned earlier in Section 4.1. Conversion to the new exception mechanism allows more than 200 lines of code to be removed from class \texttt{Pretty} (~1,000 LOC), and more importantly, restores static checking.

• Using only checked exceptions, we managed to reimplement the \texttt{EasyIo} text parsing package\footnote{\url{www.cs.cornell.edu/courses/cs2112/2015fa/#Libraries}} that was developed for a Cornell programming course. This codebase (~1,000 LOC) uses exceptions heavily for backtracking.

9.2 Performance

The current Genus implementation targets Java. We explored its performance through several experiments. All data were collected using Java 8 on a 3.4GHz Intel Core i7 processor after warming up the HotSpot JVM.

\textit{Performance of normal-case code}. Perhaps the most important performance consideration for an exception mechanism is whether it slows down normal-case code. To evaluate this, we ported Java code that only uses exceptions lightly—specifically, the JOlden benchmarks [Cahoon and McKinley 2001] and, representing larger applications, the SunFlow benchmark [SunFlow] from the DaCapo suite [Blackburn et al. 2006]. SunFlow is a ray tracer containing ~200 classes and ~21K LOC.

To evaluate the overhead of the new exception mechanism fairly, we compared the running times of this code between the extended Genus language (Section 8) and the base Genus language. Despite support for reified generics, the performance under base Genus is close to Java: compared to Java, it incurred a slowdown of 0.3%.

Figure 18 reports the results of this comparison. Each reported measurement averages at least 20 runs, with a standard error less than 1.2%. Benchmark parameters were set so that each run took more than 30 seconds.

Overall, the extended compiler generates slightly faster code than the original compiler. The average speedup is 2.4%, though performance varies by benchmark. The Health benchmark runs significantly faster on average because of the exception-based translation of enhanced \texttt{for} loops.

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{performance.png}
\caption{Performance of the exception mechanism on the JOlden benchmarks and SunFlow.}
\end{figure}
Table 1: Performance with EasyIO (ms)

<table>
<thead>
<tr>
<th>mechanism</th>
<th>exception mechanism</th>
<th>time (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Java exceptions</td>
<td>new instance</td>
<td>817.7</td>
</tr>
<tr>
<td>Java exceptions</td>
<td>cached</td>
<td>124.7</td>
</tr>
<tr>
<td>unchecked wrappers</td>
<td>cached</td>
<td>826.0</td>
</tr>
<tr>
<td>Genus exceptions</td>
<td>new instance</td>
<td>139.8</td>
</tr>
<tr>
<td>Genus exceptions</td>
<td>cached</td>
<td>128.6</td>
</tr>
</tbody>
</table>

Table 2: Exception tunneling microbenchmarks (ns)

Performance of exception-heavy code. To evaluate the performance improvement that Genus obtains by avoiding stack capture on realistic code, we measured the running times of pattern-matching regular expressions using the EasyIO package. It makes heavy use of exceptions to control search. The running times (in ms) of each pass are shown in Table 1. Each number averages 10 runs, and each run performs 1,000 passes on the input, with 6,235 exceptions thrown in each pass.

Stack capture in Java causes more than $6 \times$ overhead compared to Genus exceptions. Genus targets Java, so it is not surprising that good performance can be achieved with Java, if stack capture is turned off and exception objects are cached.

Exception tunneling performance. We used a microbenchmark to explore the overhead of exception tunneling, the key difference between Genus and Java. The microbenchmark performs method calls on objects passed down from a higher-order function; the method call either throws an exception or returns immediately. Since there is no other work done by the method, performance differences are magnified.

The results are shown in Table 2. We compare exception tunneling in Genus to two (unsafe) Java workarounds: typical Java exceptions and unchecked-exception wrappers. We also refine the comparison for typical Java exceptions and tunneled Genus exceptions based on whether a new exception object is created for each throw; throwing a single cached instance is a reasonable approach for non-failure exceptions carrying no extra information. Each number averages 20 runs, with a standard error less than 0.6% of the mean.

The rightmost column measures time to exit via an exception. Genus exceptions perform well because they do not capture the stack. The slowdown compared to the second row is mostly from borrow and handback calls (Section 8) that happen in every loop iteration because of exception mismatch.

On the other hand, Genus exceptions significantly outperform unchecked wrappers, the safest way to tunnel in Java. Java’s performance is poor here because an unchecked-exception object is created for each raised exception, whereas the implementation of Genus recycles blame objects.

The microbenchmark also measures the time to return from a method normally. The average cost of a call and return in Java was 6.0 ns. In the absence of mismatch, our translation adds the overhead of passing a null pointer to the normal return path, increasing the cost slightly to 6.3 ns. The results in Figure 18 suggest this increase is negligible in practice.

10 Related Work

Notable approaches to exceptions. PL/I was the first language with exceptions. It supports user-defined exceptions with exception handlers dynamically bound to exceptions [MacLaren 1977]. Goodenough [1975] and Liskov and Snyder [1979] introduced statically scoped handlers. CLU [Liskov and Snyder 1979] was the

**Empirical findings.** An empirical study by Cabral and Marques [2007a] shows that in Java and .NET exception handlers are not specialized enough to allow effective handling, which we believe is partly attributable to a lack of documentation of exceptions in the .NET case [Cabral and Marques 2007b] and the rigidity of checked exceptions in the Java case. Robillard and Murphy [2000] identify the global reasoning required of programmers as a major reason why exceptions are hard to use.

**Exception analysis.** Function types in functional languages such as ML and Haskell do not include exceptions because they would interfere with the use of higher-order functions. Exception capture can be avoided in SML [Milner et al. 1990] because exception types are generative, but other variants of ML lack this feature. Leroy and Pessaux [2000] observe that uncaught exceptions are the most common failure mode of large ML applications, motivating them and others [Fähndrich et al. 1998] to develop program analyses to infer exceptions. Such analyses can be helpful, especially for usage studies [Weimer and Necula 2008], but they necessarily involve trading off performance and precision, and entail non-local reasoning that does not aid programmers in reasoning about their code. A benefit of our mechanism is that it is likely to lead to more accurate, scalable static analyses, because precise exceptions largely remove the need to approximate exceptional control flow [Sinha and Harrold 2000; Bravenboer and Smaragdakis 2009].

**Exception polymorphism.** Some recent designs attempt to address the rigidity of checked exceptions through exception polymorphism: anchored exceptions [van Dooren and Steegmans 2005] as a Java extension, polymorphic effects [Rytz et al. 2012] as a Scala extension, row-polymorphic effect types in the Koka language [Leijen 2014], and the rethrows clause introduced in Swift 2 [Swift 2014]. These approaches add annotation burden to exception-oblivious code; more fundamentally, they do not address exception capture.

**Blame tracking.** Our notion of blame is related to that introduced by work on contracts [Findler and Felleisen 2002] and further developed by work on gradual typing [Wadler and Findler 2009], in which blame indicates where fault lies in the event of a contract violation (or cast failure). In our setting, an exception mismatch results in static blame being assigned that indicates where “fault” lies should an exception arise at run time, with the compiler statically checking that the “faulty” program point handles exceptions.

Blame has polarity [Findler and Felleisen 2002; Wadler and Findler 2009]; in our setting, exception mismatch at covariant (or contravariant) positions gives rise to positive (or negative) blame. Existing mechanisms for checked exceptions only consider positive blame; exceptions with negative blame are the missing piece. By contrast, in Genus both kinds of exceptions are subject to static checking, and our implementation and formalization manifest their difference: exceptions with negative blame acquire new identities to achieve safe tunneling.

**Type inference.** Our exactness inference bears resemblance to work on gradual type inference [Rastogi et al. 2012]. Both inference algorithms encode escape analysis “for free”, although the motivation for escape analysis differs. Our approach to default exactness (Section 6.1) is similar to default region annotations in a region-based type system [Grossman et al. 2002].
11 Conclusions

We have introduced a new exception mechanism that combines the benefits of static checking with the flexibility of unchecked exceptions. We were guided in the design of this mechanism by thinking carefully about the goals of an exception mechanism, by much previous work, and by many discussions found online. Our formal results suggest that our implementation offers programmers strong assurance their exceptions are handled. Our evaluation shows that the mechanism works well on real code. The exception mechanism adds negligible cost when exceptions are not being used; exception tunneling comes with a small performance penalty that appears to be more than offset in practice by avoiding the run-time overhead of wrapping exceptions. In short, we believe we have identified a promising approach for the design of future exception mechanisms.

Acknowledgments

We thank Owen Arden, Chinawat Isradisaikul, Jed Liu, Michael Hicks, and the anonymous reviewers for discussions about exception mechanisms and for suggestions about this paper. This research has been supported by MURI grant FA9550-12-1-0400, administered by the US Air Force, by NSF grant 1513797, and by the European Research Council, grant No. 321217. This paper does not necessarily reflect the views of any of its sponsors.

References


Apache Commons. The Apache Commons project. https://commons.apache.org/.


M. van Dooren and E. Steegmans. Combining the robustness of checked exceptions with the flexibility of unchecked exceptions using anchored exception declarations. In *20th ACM SIGPLAN Conf. on Object-Oriented Programming, Systems, Languages and Applications (OOPSLA)*, 2005.


A Proving CBC Type-Safe

This appendix proves the main results of Section 7.

Theorem 1 (Kernel soundness: preservation and progress)
- If \( \emptyset; K \vdash e : [T]_U \) and \( e \rightarrow e' \) then \( \emptyset; K \vdash e' : [T]_{U'} \).
- If \( \emptyset; K \vdash e : [T]_{U'} \) then either
  1. \( \exists v. e = v, \) or
  2. \( \exists U_0 \in \overline{U}, e = \text{throw } U_0, \) or
  3. \( \exists e'. e \rightarrow e' \).

Proof. We prove preservation first.

Case 1 \( e = (\lambda x : T_1.e_1) v \) and \( e \rightarrow e_1\{v/x\} \) via Beta. The typing derivation of \( e \) looks like the following:

\[
\begin{array}{ccc}
\varnothing; \top \vdash \lambda x : T_1.e_1 : [T]_U & \varnothing; K \vdash v : [S_2]_{U'} & S_2 \preceq_{[T]} T_1 \\
\end{array}
\]

Given the above type judgment for \( e_1 \), by Lemma 3, we have \( x : T_1(\overline{U}_2); \top \vdash e_1 : [S_1]_{U_1 \cup \overline{U}_2} \).

By Lemma 2, \( \varnothing; \top \vdash e_1\{v/x\} : [S_1]_{U_1 \cup \overline{U}_2} \). By Lemma 5, \( \varnothing; K \vdash e_1\{v/x\} : [S_1]_{U_1 \cup \overline{U}_2} \).

Case 2 \( e = (\text{let } x : T_1 \leftarrow v \text{ in } e_1) \) and \( e \rightarrow e_1\{v/x\} \) via Let. The typing derivation of \( e \) looks like the following:

\[
\begin{array}{ccc}
\varnothing; K (T_1) \vdash v : [S_1]_{\emptyset} & x : T_1(\overline{U}_1); K \vdash e_1 : [T]_{U'} & S_1 \preceq_{[T]} T_1 \\
\end{array}
\]

By Lemma 2, \( \varnothing; K \vdash e_1\{v/x\} : [T]_{U'} \).

Case 3 \( e = \text{try } v \text{ catch } U' \triangleright e_2 \) and \( e \rightarrow v \) via Try. The typing derivation of \( e \) looks like the following:

\[
\begin{array}{ccc}
\varnothing; K \vdash v : [T]_{\emptyset} & \varnothing; K \vdash e_2 : [T]_{U'} & \varnothing \subseteq \overline{U}' \\
\end{array}
\]

So \( \varnothing; K \vdash v : [T]_{U'} \) follows from T-SUBSUME.

Case 4 \( e = \text{try throw } U' \text{ catch } \ldots U' \triangleright e' \ldots \) and \( e \rightarrow e' \) via Catch. The typing derivation of \( e \) looks like the following:

\[
\begin{array}{ccc}
\varnothing; K \vdash \text{throw } U' : [T]_{U'} & \varnothing; K \vdash e' : [T]_{U'} & \ldots \\
\end{array}
\]

The result follows.

Case 5 \( e = C[\text{throw } U'] \) where \( \text{throw } U' \in C \), and thus \( e \rightarrow \text{throw } U' \) via Throw. By Lemma 6, \( U' \in \overline{U} \). Additionally, there exists \( S \) such that \( S \preceq_{\emptyset} T \) and \( \Delta; K \vdash \text{throw } U' : [S]_{U'} \). Thus the result follows from T-SUBSUME.
Case 6 $e = C[e_0]$ and $e_0 \rightarrow e'_0$, and thus $e \rightarrow C[e'_0]$ via CONTEXT. In this case, the result can be obtained by induction on the typing derivation of $e$.

Next we prove progress, by induction on the typing derivation of $e$.

Case 1 $e = b$. The result is trivial.

Case 2 $e = x$. This case is impossible because the environment contains no mapping for $x$.

Case 3 $e = \lambda x : T_1 . e_1$. The result is trivial.

Case 4 $e = e_1 e_2$. In this case, since $e$ has a typing derivation, we know there are typing derivations for $e_1$ and $e_2$ as well. The induction hypotheses they provide say that each of $e_1$ and $e_2$ is either a value, a throw, or a term that is able to take a step.

Case 4.1 $e_1$ is a value.

Case 4.1.1 $e_2$ is a value. In this case $e_1$ must be an abstraction. BETA allows $e$ to step.

Case 4.1.2 $e_2$ is a throw. THROW allows $e$ to step.

Case 4.1.3 $e_2$ steps. CONTEXT allows $e$ to step.

Case 4.2 $e_1$ is a throw. THROW allows $e$ to step.

Case 4.3 $e_1$ steps. CONTEXT allows $e$ to step.

Case 5 $e = \text{let } x : T_1 \leftarrow e_1 \text{ in } e_2$. By induction, we know $e_1$ is either a value, a throw, or a term that is able to take a step.

Case 5.1 $e_1$ is a value. LET allows $e$ to step.

Case 5.2 $e_2$ is a throw. THROW allows $e$ to step.

Case 5.3 $e_1$ steps. CONTEXT allows $e$ to step.

Case 6 $e = \text{throw } U_0$. The result trivially holds.

Case 7 $e = \text{try } e_1 \text{ catch } U' e_2$. By induction, we know $e_1$ is either a value, a throw, or a term that is able to take a step.

Case 7.1 $e_1$ is a value. TRY allows $e$ to step.

Case 7.2 $e_2 = \text{throw } U''$.

Case 7.2.1 $U'' \in U'$. CATCH allows $e$ to step.

Case 7.2.2 $U'' \notin U'$. THROW allows $e$ to step.

Case 7.3 $e_1$ steps. CONTEXT allows $e$ to step.

Lemma 2 (Substitution Lemma)

$$\Delta, x : T(U); K \vdash e : [T']_{U'} \wedge \varnothing ; K' \vdash v : [S]_\varnothing \wedge \understack{S \triangleleft_{T'} \ T \implies \Delta; K \vdash e \{ v/x \} : [T']_{U'}}$$

Proof. By induction on the type derivation of $e$.

Case 1 $e = b$. The result is trivial in this case.

Case 2 $e$ is a variable.
Case 2.1 \( e = x \). Then \( e\{v/\} = v \).

**Case 2.1.1** \( T \) is strong. In this case the type derivation of \( e \) is obtained via T-VAR-S. So \( T' = S \) and \( \overline{U'} = \emptyset \). Given the type judgment for \( v \), we can obtain \( \emptyset; K \vdash e\{v/\} : [S]_\emptyset \) by Lemma 4. The result then follows by weakening the variable environment.

**Case 2.1.2** \( T \) is weak. In this case the type derivation of \( e \) looks like the following

\[
\frac{x: T_1 \vdash [S_1]_{\overline{T}_1}(\overline{U}_1)}{\Delta, x: T_1 \vdash [S_1]_{\overline{T}_1}(\overline{U}_1); K \vdash x : T_1 \vdash [S_1]_{\overline{T}_1 \cup \overline{U}_1}}
\]

So \( T = T_1 \vdash [S_1]_{\overline{T}_1}, T' = T_1 \vdash [S_1]_{\overline{T}_1 \cup \overline{U}_1}, \) and \( \overline{U} = \emptyset \).

By \( S \lesssim_U T \) and \( \emptyset; K' \vdash v : [S]_\emptyset \), we have \( \emptyset; K' \vdash v : \left[ T_1 \vdash [S_1]_{\overline{T}_1 \cup \overline{U}_1} \right]_\emptyset \).

Thus \( \emptyset; K \vdash v : \left[ T_1 \vdash [S_1]_{\overline{T}_1 \cup \overline{U}_1} \right]_\emptyset \) by Lemma 4.

The result then follows by weakening the variable environment.

**Case 2.2** \( e = y \neq x \). Then \( e\{v/\} = e \). Therefore the result trivially holds.

**Case 3** \( e = \lambda y : T_1 . e_1 \). The type derivation of \( e \) looks like the following

\[
\frac{\Delta, x : T(\overline{U}), y : T_1(\emptyset); K \vdash e_1 : [S_1]_{\overline{T}_1}}{\Delta, x : T(\overline{U}); K \vdash \lambda y : T_1 . e_1 : \left[ T_1 \vdash [S_1]_{\overline{T}_1} \right]_\emptyset}
\]

So \( T' = T_1 \vdash [S_1]_{\overline{T}_1} \) and \( \overline{U'} = \emptyset \).

**Case 3.1** \( x = y \). In this case \( e_1\{v/\} = e_1 \) and \( \Delta, x : T(\overline{U}), y : T_1(\emptyset) = \Delta, y : T_1(\emptyset) \). So we have

\[
\Delta, y : T_1(\emptyset); K \vdash e_1\{v/\} : [S_1]_{\overline{T}_1}
\]

This implies the result via T-ABS.

**Case 3.2** \( x \neq y \). In this case the type judgment for \( e_1 \) gives the following induction hypothesis

\[
\Delta, y : T_1(\emptyset); K \vdash e_1\{v/\} : [S_1]_{\overline{T}_1}
\]

This implies the result via T-ABS.

**Case 4** \( e = e_1 \ e_2 \). The type derivation of \( e \) looks like the following

\[
\Delta, x : T(\overline{U}); \top \vdash e_1 : \left[ T_1 \vdash [S']_{\overline{T}_3} \right]_{\overline{T}_1} \quad \Delta, x : T(\overline{U}); K(\top) \vdash e_2 : [T_2]_{\overline{T}_2} \quad T_2 \lesssim_{\overline{U}_2} T_1
\]

So \( T' = S' \) and \( \overline{U'} = \overline{T}_1 \cup \overline{T}_2 \cup \overline{T}_3 \cup \overline{U}_2 \). The induction hypotheses are

\[
\Delta; \top \vdash e_1\{v/\} : \left[ T_1 \vdash [S']_{\overline{T}_3} \right]_{\overline{T}_1} \quad \text{and} \quad \Delta; K(\top) \vdash e_2\{v/\} : [T_2]_{\overline{T}_2}
\]

which imply

\[
\Delta; K \vdash e_1\{v/\} \ e_2\{v/\} : [S']_{\overline{T}_1 \cup \overline{T}_2 \cup \overline{T}_3 \cup \overline{U}_2}
\]

via T-APP.
Case 5  \( e = \text{let } y : T_1 \leftarrow e_1 \text{ in } e_2 \). The type derivation of \( e \) looks like the following

\[
\frac{\Delta, x : T(\overline{U}); K(T_1) \vdash e_1 : [T_3]_{\overline{U'}}}{T_3 \preceq_{\overline{U'}} T_1} \quad \frac{\Delta, x : T(\overline{U}), y : T_1(\overline{U''}); K(T_1) \vdash e_2 : [T_2]_{\overline{U_2'}}}{\Delta, x : T(\overline{U}); K \vdash \text{let } y : T_1 \leftarrow e_1 \text{ in } e_2 : [T_2]_{\overline{U_1} \cup \overline{U_2'}}}
\]

So \( T' = T_2 \) and \( \overline{U'} = \overline{U_1} \cup \overline{U_2} \).

The type judgment for \( e_1 \) gives the following induction hypothesis

\[
\Delta ; K(T_1) \vdash e_1 \{v/x\} : [T_3]_{\overline{U_1}}
\]

Case 5.1 \( x = y \). In this case \( e_2 \{x/v\} = e_2 \) and \( \Delta, x : T(\overline{U}), y : T_1(\overline{U''}) = \Delta, y : T_1(\overline{U''}) \). So we have

\[
\Delta, y : T_1(\overline{U''}); K(T_1) \vdash e_2 \{v/x\} : [T_2]_{\overline{U_2'}}
\]

Thus the result follows from T-LET.

Case 5.2 \( x \neq y \). In this case the type judgment for \( e_2 \) gives the following induction hypothesis

\[
\Delta, y : T_1(\overline{U''}); K(T_1) \vdash e_2 \{v/x\} : [T_2]_{\overline{U_2'}}
\]

Thus the result follows from T-LET.

Case 6  \( e = \text{throw } U \). The result is trivial in this case.

Case 7  \( e = \text{try } e_1 \text{ catch } U_0 \triangleright e_2 \). The type derivation of \( e \) looks like the following

\[
\frac{\Delta, x : T(\overline{U}); K \vdash e_1 : [T']_{\overline{U_1}}}{\Delta, x : T(\overline{U}); K \vdash \text{try } e_1 \text{ catch } U_0 \triangleright e_2 : [T']_{(\overline{U_1} \setminus U_0) \cup \overline{U_2}}}
\]

So \( \overline{U'} = (\overline{U_1} \setminus U_0) \cup \overline{U_2} \). Since \( e \{v/x\} = \text{try } e_1 \{v/x\} \text{ catch } U_0 \triangleright e_1 \{v/x\} \), the result can be obtained by using the induction hypotheses.

Lemma 3 (Exception polymorphism)

Given variable environment \( \Delta \) and a fixed set of exceptions \( \overline{U'} \). Let \( \Delta' \) be the variable environment that augments the exceptions associated with each variable in \( \Delta \) with \( \overline{U'} \), that is

\[
\Delta' = \{ x : T(\overline{U} \cup \overline{U'}) \mid x : T(\overline{U}) \in \Delta \}. \]

Then

(i) \( \Delta_0, \Delta; \bot \vdash e_0 : [T_0]_{\overline{U_0}} \implies \Delta_0, \Delta'; \bot \vdash e_0 : [T_0]_{\overline{U_0} \cup \overline{U'}} \)

(ii) \( \Delta_0, \Delta; \top \vdash e_0 : \left[ T_0 \xrightarrow{K_0} [S_0']_{\overline{U_0} \cup \overline{U'}} \right]_{\overline{U_0}} \implies \Delta_0, \Delta'; \top \vdash e_0 : \left[ T_0 \xrightarrow{K_0} [S_0']_{\overline{U_0} \cup \overline{U'}} \right]_{\overline{U_0} \cup \overline{U'}} \)

Proof. For any \( x : T(\overline{U}) \in \Delta \), if \( T \) is a strong type, then \( \overline{U} \) and \( \overline{U'} \) must both be \( \varnothing \), and thus the results hold trivially. So in the following we assume such \( T \)’s are weak and prove the results by induction on the type derivation of \( e_0 \). We will use \( \Delta_{-y} \) to denote \{ \( x : T(\overline{U}) \mid x : T(\overline{U}) \in \Delta \) and \( x \neq y \) \}.

Case 1  \( e_0 = b \). The results hold trivially in this case.

32
Case 2  $e_0 = x$. In this case $\mathcal{U}_0 = \emptyset$.

Case 2.1  $x \in \text{dom}(\Delta)$. Suppose $x : T(\mathcal{U}) \in \Delta$. Notice that (i) is impossible because $x : T(\mathcal{U}) \not\in (\Delta, x : T(\mathcal{U}))_\perp$ as $T$ is weak. The type derivation of $e_0$ is

$$
x : T'_0 \vdash [S'_0]_{\mathcal{U}'_0} \in (\Delta_0, \Delta)_T
$$

$$
\Delta_0, \Delta ; T \vdash x : [T'_0 \vdash [S'_0]_{\mathcal{U}'_0}]_{\emptyset}
$$

So $T = T'_0 \vdash [S'_0]_{\mathcal{U}'_0}$ and $\mathcal{U}'_0 = \emptyset \cup \mathcal{U}$. The result (ii) then can be obtained via T-VAR-W:

$$
x : T'_0 \vdash [S'_0]_{\mathcal{U}'_0} \cup \mathcal{U} \in (\Delta_0, \Delta')_T
$$

$$
\Delta_0, \Delta'; T \vdash x : [T'_0 \vdash [S'_0]_{\mathcal{U}'_0} \cup \mathcal{U}']_{\emptyset}
$$

Case 2.2  $x \notin \text{dom}(\Delta)$. The results hold trivially in this case.

Case 3  $e_0 = \lambda y : T_1 . e_1$. The type derivation of $e_0$ looks like the following

$$
(\Delta_0, \Delta)_K, y : T_1(\mathcal{U}); \perp \vdash e_1 : [S_1]_{\mathcal{U}'_1}
$$

$$
\Delta_0, \Delta ; K \vdash \lambda y : T_1 . e_1 : [T_1 \vdash [S_1]_{\mathcal{U}'_1}]_{\emptyset}
$$

Case 3.1  $K = \perp$. Then $(\Delta_0, \Delta)_K = (\Delta_0)_K = (\Delta_0, \Delta')_K$ as $\Delta_\perp = \Delta'_\perp = \emptyset$. The result (i) then follows from T-ABS.

Case 3.2  $K = \top$.

Case 3.2.1  $y \in \text{dom}(\Delta)$. Then $(\Delta_0, \Delta)_K, y : T_1(\mathcal{U}) = (\Delta_0)_K, y : T_1(\mathcal{U}), \Delta_y$. So the induction hypothesis is

$$
(\Delta_0)_K, y : T_1(\mathcal{U}), \Delta'_y; \perp \vdash e_1 : [S_1]_{\mathcal{U}'_1} \cup \mathcal{U}'
$$

Since $(\Delta_0)_K, y : T_1(\mathcal{U}), \Delta'_y = (\Delta_0, \Delta')_K, y : T_1(\mathcal{U})$, we can obtain $\Delta_0, \Delta'; K \vdash \lambda y : T_1 . e_1 : [T_1 \vdash [S_1]_{\mathcal{U}'_1} \cup \mathcal{U}']_{\emptyset}$ via T-ABS. So the result (ii) holds.

Case 3.2.2  $y \notin \text{dom}(\Delta)$. Then we can use the induction hypothesis to obtain $\Delta_0, \Delta'; K \vdash \lambda y : T_1 . e_1 : [T_1 \vdash [S_1]_{\mathcal{U}'_1} \cup \mathcal{U}']_{\emptyset}$. So the result (ii) holds.

Case 4  $e_0 = e_1 e_2$. The type derivation of $e_0$ looks like the following

$$
\Delta_0, \Delta ; \top \vdash e_1 : [T_1 \vdash [S_1]_{\mathcal{U}'_1}]_{\mathcal{U}_1} \quad \Delta_0, \Delta ; K(T_1) \vdash e_2 : [T_2]_{\mathcal{U}_2} \quad T_2 \leq_{\mathcal{U}'} T_1
$$

So $\mathcal{U}_0 = \mathcal{U}_1 \cup \mathcal{U}_2 \cup \mathcal{U}_3 \cup \mathcal{U}'$. The type judgment for $e_1$ gives rise to the following induction hypothesis

$$
\Delta_0, \Delta'; \top \vdash e_1 : [T_1 \vdash [S_1]_{\mathcal{U}'_1} \cup \mathcal{U}']_{\mathcal{U}_1 \cup \mathcal{U}'}
$$

Case 4.1  $K(T_1) = \perp$. In this case the induction hypothesis given by the type judgment for $e_2$ is

$$
\Delta_0, \Delta'; \perp \vdash e_2 : [T_2]_{\mathcal{U}_2 \cup \mathcal{U}'}
$$

So it can be obtained via T-APP that $\Delta_0, \Delta'; K \vdash e_1 e_2 : [S_1]_{\mathcal{U}_3 \cup \mathcal{U}_2 \cup \mathcal{U}_3 \cup \mathcal{U}'}$. The results (i) and (ii) then follow.
Case 4.2 \( K(1) = \top \). In this case the induction hypothesis given by the type judgment for \( e_2 \) is
\[
\Delta_0, \Delta'; \top \vdash e_2 : [T'_2]_{\mathcal{T}_2 \cup \mathcal{U}}
\]

where \( T'_2 = T_2 \overset{\kappa_2}{\rightarrow} [S_2]_{\mathcal{T}_2 \cup \mathcal{U}} \) given that \( T_2 = T_2 \overset{\kappa_2}{\rightarrow} [S_2]_{\mathcal{T}_2} \). This implies \( T'_2 \preceq_{\mathcal{T}_2 \cup \mathcal{U}} T_1 \). So it can be obtained via \( \mathcal{T} \text{-App} \) that \( \Delta_0, \Delta'; K \vdash e_1, e_2 : [S_1]_{\mathcal{T}_2 \cup \mathcal{U}} \). The results (i) and (ii) then follow.

Case 5 \( e_0 = \text{let } y : T_1 \leftarrow e_1 \text{ in } e_2 \). The type derivation of \( e_0 \) looks like the following
\[
\Delta_0, \Delta; K(1) \vdash e_1 : [T_3]_{\mathcal{T}_3} \quad T_3 \preceq_{\mathcal{T}_3 \cup \mathcal{U}} T_1 \quad \Delta_0, \Delta; y : T_1(\mathcal{U}) ; K \vdash e_2 : [T_2]_{\mathcal{T}_2}
\]

The type judgment for \( e_1 \) gives rise to the following induction hypothesis
\[
\Delta_0, \Delta'; K(1) \vdash e_1 : [T'_3]_{\mathcal{T}_3}
\]

where \( T'_3 \preceq_{\mathcal{T}_3 \cup \mathcal{U}} T_1 \) when \( K(1) = \bot \), and \( T'_3 \preceq_{\mathcal{T}_3 \cup \mathcal{U}} T_1 \) when \( K(1) = \top \).

Case 5.1 \( K = \bot \).

Case 5.1.1 \( y \in \text{dom}(\Delta) \). In this case, \( \Delta_0, \Delta, y : T_1(\mathcal{U}) = \Delta_0, y : T_1(\mathcal{U}), \Delta_{\neg y} \).

Case 5.1.1.1 \( K(1) = \bot \). The result (i) can be obtained using the following induction hypothesis
\[
\Delta_0, y : T_1(\mathcal{U}), \Delta_{\neg y} ; \bot \vdash e_2 : [T_2]_{\mathcal{T}_2 \cup \mathcal{U}}
\]

Case 5.1.2 \( K(1) = \top \). The result (i) can be obtained using the following induction hypothesis
\[
\Delta_0, y : T_1(\mathcal{U} \cup \mathcal{U}), \Delta_{\neg y} ; \bot \vdash e_2 : [T_2]_{\mathcal{T}_2 \cup \mathcal{U}}
\]

Case 5.1.2.1 \( y \notin \text{dom}(\Delta) \).

Case 5.1.2.1.1 \( K(1) = \bot \). The result (i) can be obtained using the following induction hypothesis
\[
\Delta_0, y : T_1(\mathcal{U}), \Delta' ; \bot \vdash e_2 : [T_2]_{\mathcal{T}_2 \cup \mathcal{U}}
\]

Case 5.1.2.2 \( K(1) = \top \). The result (i) can be obtained using the following induction hypothesis
\[
\Delta_0, \Delta', y : T_1(\mathcal{U} \cup \mathcal{U}) ; \bot \vdash e_2 : [T_2]_{\mathcal{T}_2 \cup \mathcal{U}}
\]

Case 5.2 \( K = \top \). In this case we know \( T_2 = T_0 \overset{\kappa_0}{\rightarrow} [S_0]_{\mathcal{T}_0} \).

Case 5.2.1 \( y \in \text{dom}(\Delta) \). In this case, \( \Delta_0, \Delta, y : T_1(\mathcal{U}) = \Delta_0, y : T_1(\mathcal{U}), \Delta_{\neg y} \).

Case 5.2.1.1 \( K(1) = \bot \). The result (ii) can be obtained using the following induction hypothesis
\[
\Delta_0, y : T_1(\mathcal{U}), \Delta_{\neg y} ; \top \vdash e_2 : \left[ T'_0 \overset{\kappa'_0}{\rightarrow} [S'_0]_{\mathcal{T}_0} \cup \mathcal{U} \right]_{\mathcal{T}_0 \cup \mathcal{U}}
\]

Case 5.2.1.2 \( K(1) = \top \). The result (ii) can be obtained using the following induction hypothesis
\[
\Delta_0, y : T_1(\mathcal{U} \cup \mathcal{U}), \Delta_{\neg y} ; \top \vdash e_2 : \left[ T'_0 \overset{\kappa'_0}{\rightarrow} [S'_0]_{\mathcal{T}_0} \cup \mathcal{U} \right]_{\mathcal{T}_0 \cup \mathcal{U}}
\]

Case 5.2.2 \( y \notin \text{dom}(\Delta) \).
Case 5.2.2.1 \( K(T_1) = \bot \). The result (ii) can be obtained using the following induction hypothesis

\[
\Delta_0, y : T_1(\overline{U''}), \Delta' ; T \vdash e_2 : \left[ T_0' \xrightarrow{\Delta_0} [S_0']_{U_0' \cup U''} \right]_{U_2 \cup U_0''}
\]

Case 5.2.2.2 \( K(T_1) = \top \). The result (ii) can be obtained using the following induction hypothesis

\[
\Delta_0, \Delta' ; y : T_1(\overline{U''} \cup \overline{U'}) ; T \vdash e_2 : \left[ T_0' \xrightarrow{\Delta_0} [S_0']_{U_0' \cup U''} \right]_{U_2 \cup U_0''}
\]

Case 6 \( e_0 = \text{throw } U \). The results (i) and (ii) hold trivially in this case.

Case 7 \( e_0 = \text{try } e_1 \text{ catch } U'' \triangleright e_2 \). The type derivation of \( e_0 \) looks like the following.

\[
\Delta_0, \Delta ; K \vdash e_1 : [T_0]_{\overline{U_1}} \quad \Delta_0, \Delta ; K \vdash e_2 : [T_0]_{\overline{U_2}} \quad U'' \subseteq \overline{U_1}
\]

\[
\Delta_0, \Delta ; K \vdash \text{try } e_1 \text{ catch } U'' \triangleright e_2 : [T_0]_{(\overline{U_1} \cup \overline{U''}) \cup \overline{U_2}}
\]

Case 7.1 \( K = \bot \). The induction hypotheses are \( \Delta_0, \Delta' ; K \vdash e_1 : [T_0]_{\overline{U_1} \cup \overline{U'}} \) and \( \Delta_0, \Delta' ; K \vdash e_2 : [T_0]_{\overline{U_2} \cup \overline{U''}} \). So the result (i) can be obtained via \text{T-TRY-\text{CATCH}}.

Case 7.2 \( K = \top \). The induction hypotheses are \( \Delta_0, \Delta' ; K \vdash e_1 : [T_0']_{\overline{U_1} \cup \overline{U''}} \) \[ [S_0']_{U_0' \cup U''} \]

and \( \Delta_0, \Delta' ; K \vdash e_2 : [T_0']_{\overline{U_1} \cup \overline{U''}} \), supposing \( T_0 = T_0' \xrightarrow{K_0'} [S_0']_{U_0''} \). So the result (ii) can be obtained via \text{T-TRY-\text{CATCH}}.

Lemma 4 \( \varnothing ; K \vdash v : [S]_{\overline{U}} \implies \varnothing ; K' \vdash v : [S]_{\overline{U}} \).

Proof. The result is trivial if \( K = K' \). Below we assume \( K \neq K' \).

Case 1 \( v = b \). The result is trivial in this case.

Case 2 \( v = \lambda x : T_1 \vdash e_1 \). Let \( S \) be \( T_1 \vdash [S_1]_{\overline{U_1}} \). From the typing derivation of \( v \), we know \( x : T_1(\varnothing) ; \bot \vdash e_1 : [S_1]_{\overline{U_1}} \). Notice that \( \varnothing_K = \varnothing_{K'} = \varnothing \). The result then follows from \text{T-ABS}.

Lemma 5 \( \Delta ; \bot \vdash e : [S]_{\overline{U}} \implies \Delta ; T \vdash e : [S]_{\overline{U}} \).

Proof. By induction on the typing derivation of \( e \).

Case 1 \( e = b \). The result is trivial in this case.

Case 2 \( e = x \). The typing of \( e \) must be derived using \text{T-VAR-S}. It looks like the following:

\[
\begin{align*}
x : S(\varnothing) & \in \Delta_\bot \\
\Delta ; \bot & \vdash x : [S]_{\varnothing}
\end{align*}
\]

So \( x : S(\varnothing) \in \Delta_\bot \subseteq \Delta_T \) and the result follows.
Case 3 $e = \lambda x : T_1 \cdot e_1$. The typing of $e$ looks like the following:

$$\Delta_\perp, x : T_1(\emptyset); \perp \vdash e_1 : [S_1]_{\Gamma_1^-}$$

$$\Delta; \perp \vdash \lambda x : T_1 \cdot e_1 : [T_1 \vdash [S_1]_{\Gamma_1^-}]_\emptyset$$

So $S = T_1 \vdash [S_1]_{\Gamma_1^-}$. The induction hypothesis is $\Delta_\perp, x : T_1(\emptyset); \top \vdash e_1 : [S_1]_{\Gamma_1^-}$. Since $\Delta_\perp \subseteq \Delta_\top$, we can weaken the environment and obtain $\Delta_\top, x : T_1(\emptyset); \top \vdash e_1 : [S_1]_{\Gamma_1^-}$. The result then follows from T-Abs.

Case 4 $e = e_1 e_2$. The typing of $e$ looks like the following:

$$\Delta; \top \vdash e_1 : [T_1 \vdash [S_1]_{\Gamma_1^-}]_{\Gamma_1}$$

$$\Delta; K \vdash e_1 e_2 : [S]_{\Gamma_1 \cup \Gamma_2 \cup \Gamma_3 \cup \Gamma_4}$$

$$\Delta; K \vdash e_1 : [S]_{\Gamma_1 \cup \Gamma_2 \cup \Gamma_3 \cup \Gamma_4}$$

which is independent of $K$. The result holds trivially.

Case 5 $e = \text{let } x : T_1 \leftarrow e_1 \text{ in } e_2$. The typing of $e$ looks like the following:

$$\Delta; K(1) \vdash e_1 : [T_1 \vdash [S_1]_{\Gamma_1^-}]_{\Gamma_1^-}$$

$$T_3 \vdash_{\Gamma_1^-} T_1$$

$$\Delta; \top \vdash x : T_1 \leftarrow e_1 \text{ in } e_2 : [S]_{\Gamma_1 \cup \Gamma_2}$$

The induction hypothesis provided by the typing of $e_2$ is $\Delta; x : T_1(\emptyset); \top \vdash e_2 : [S]_{\Gamma_2}$. The result then follows via T-Let.

Case 6 $e = \text{throw } U_0$. The result is trivial in this case.

Case 7 $e = \text{try } e_1 \text{ catch } \overline{U} \triangleright e_2$. The typing of $e$ looks like the following:

$$\Delta; \top \vdash e_1 : [S]_{\Gamma_1^-}$$

$$\Delta; \top \vdash e_2 : [S]_{\Gamma_2}$$

$$\overline{U} \subseteq \overline{U_1}$$

$$\Delta; \top \vdash \text{try } e_1 \text{ catch } \overline{U} \triangleright e_2 : [S]_{(\overline{U_1} \cup \overline{U})}$$

The induction hypotheses are $\Delta; \top \vdash e_1 : [S]_{\Gamma_1^-}$ and $\Delta; \top \vdash e_2 : [S]_{\Gamma_2}$. The result then follows via T-Try-Catch.

Lemma 6 $\Delta; K \vdash C[\text{throw } U'] : [T]_{\Gamma_1^-} \land \text{throw } U' \land C \implies U' \in U$

Proof. By induction on the type derivation of $C[\text{throw } U']$.

Lemma 1 (Rewriting preserves types) If $\Gamma; K \vdash f \leadsto e : [\tau]_{\Gamma_1^-}$ then $\Gamma; K \vdash e : [\tau]_{\Gamma_1^-}$.

Proof. By induction on the derivation of the translation. Most rewriting rules have a corresponding typing rule in the kernel, which causes most cases in the proof to be straightforward constructions of kernel typing derivations. The exception to this pattern is when $f$ is an application that involves mismatch. Below we show that its translation preserves the type.

Let $f$ be $\{f_1, f_2\}^\ell$. Its rewriting derivation has the following form:

$$\Gamma; \top \vdash f_1 \leadsto e_1 : [\tau_1 \vdash [\sigma_1]_{E_1}]_{E_1^-}$$

$$\Gamma; K(\tau_1) \vdash f_2 \leadsto e_2 : [\tau_2]_{E_2}$$

$$\tau_2 \vdash_{E_2} \tau_1$$

$$\tau_2 = \tau_2 \vdash_{E_2} [\tau_2]_{E_2}$$

$$\Gamma; K \vdash \{f_1, f_2\}^\ell \leadsto \text{try } e_1 \left(\text{let } x : \tau_2 \leftarrow e_2 \text{ in } \lambda y : \tau_21 \cdot \text{try } x \cdot y \text{ catch } E_\delta \triangleright \text{throw } E_\delta^\ell\right) \text{ catch } E_\delta \triangleright \text{throw } E_\delta : [\tau_1]_{E_1 \cup E_2 \cup E_3 \cup E_4}$$
The induction hypotheses are \( \Gamma; \top \vdash e_1 : [\tau_1 \rightarrow [\sigma_1]_{E_3}]_{E_1} \) and \( \Gamma; K(\tau_1) \vdash e_2 : [\tau_2]_{E_2} \). They allow the typing derivation in Figure 19, where \( \tau_2' \triangleq \tau_2 \rightarrow \sigma_{22} \rightarrow [\tau_4 \rightarrow [\sigma_{22}](E_4 \cup \delta) \cup E_5]. \)
Figure 19: The typing derivation the proof of Lemma 1 refers to